



**CITY OF DURHAM | NORTH CAROLINA**

To: Mayor and Members of the City Council

From: D. Ann Gray, MCC, NCCMC  
City Clerk

Date: December 31, 2012

Subject: Guidelines for E-mail as a Public Record In North Carolina

At the December 20, 2012 Work Session, Council Member Catotti requested additional information on managing emails.

I am attaching "Guidelines for E-mail as a Public Record" published by the North Carolina Department of Cultural Resources. Please refer to page 2 of the Table of Contents (Section 2 entitled Managing Your Inbox).

Attachment

North Carolina Department of Cultural Resources  
Division of Historical Resources  
Archives & Records Section  
Government Records Branch



Guidelines for E-mail as a Public Record in North Carolina: Tips and  
Tricks for Using Microsoft Exchange Software to Manage E-mail

Created July 2009

## **Table of Contents**

<b><u>Section 1 – Creating E-Mail Messages</u></b>	<b><u>3</u></b>
Not all E-mail Messages are Created Equal	3
Metadata: Information About the E-mail Message is Critical	4
Dealing with Threads	6
<b><u>Section 2 – Managing Your Inbox</u></b>	<b><u>7</u></b>
Managing E-Mail Messages	7
What to Keep and What to Toss	7
“Sent” E-mail Messages	8
Deleting E-Mail Messages	8
Storing and Organizing E-mail Messages	12
How Long E-Mail Messages Should be Stored	20
Organization and Storage Options Using Microsoft Outlook	20
Preserving E-mail Messages	27
File Formats	27
Storage Media	28
<b><u>Section 3 – Appropriate Use of E-mail</u></b>	<b><u>30</u></b>
Forwarding E-Mail Messages	30
E-mail Etiquette	30
Persistence	31
<b><u>Section 4 – Technical Security</u></b>	<b><u>32</u></b>
<b><u>Contact Information for Government Records</u></b>	<b><u>35</u></b>
<b><u>Appendix A</u></b>	<b><u>36</u></b>
<b><u>Bibliography</u></b>	<b><u>39</u></b>

## Section 1 – Creating E-Mail Messages

---

### Not all E-mail Messages are Created Equal ... But They Should Be.

E-mail is a convenient and quick communications tool used throughout government to collaborate and to seek and convey information. A poorly written, incomplete, or unprofessional e-mail message can result in ambiguity, misinterpretation, or negative publicity for both the agency and the creator of the message. An e-mail message containing confidential information can potentially be intercepted and read by someone who should not have access to the sensitive information, thus causing irreparable harm.

The ease of using e-mail often lure users into thinking that sending an e-mail message is like having a casual conversation with their best friend, where anything can be said without repercussion. What is often forgotten is that as a public record, the content in an e-mail message can be viewed and interpreted by those other than the sender and receiver(s). So care must be taken when composing the message to ensure it is clear, professional, and consistent.

Before you hit the "send" button, here are eight steps for composing *business* e-mail messages that will reflect you and your agency's professional reputation:<sup>1 2</sup>

1. Address your recipient by name in your salutation. Although it may be convenient to get right to your message content, don't overlook the same personal address you would use with a traditional letter. Personalizing your message indicates your level of interest in conducting business with that individual.
2. Write in complete sentences as they are much easier to read and understand than sentence fragments. Thoughtfully composed sentences reduce the need for assumptions and show your recipient that you took the time to ensure your message was communicated clearly.
3. Be brief *and* polite. If your message runs longer than two or three short paragraphs, consider reducing the message.
4. Be concise. Make sure to put your main point in the opening sentence and then quickly make your points, ask your questions or state your needs.
5. As a general rule, avoid e-mail abbreviations and chat room acronyms like LOL (laugh out loud) or organizational acronyms such as AAA (American Automobile Association). Your reader may be left wondering what you meant.
6. Resist the temptation to include or attach any confidential information. Remember, an e-mail message created, sent, or received in the course of doing business is considered to be a public record. Confidential information is protected by statute and, as such, cannot be disclosed. If e-mail messages contain both confidential and non-confidential information, and a public records request is received, an employee must provide access

---

<sup>1</sup>Adapted from Ten Tips on How to Write a Professional Email.

<http://grammar.about.com/od/developingessays/a/profemails.htm> (accessed March 1, 2009).

<sup>2</sup>Adapted from How to Compose a Professional Business Email. [http://www.ehow.com/how\\_4471941\\_compose-professional-business-email.html](http://www.ehow.com/how_4471941_compose-professional-business-email.html) (accessed March 1, 2009).

to the non-confidential information and redact the confidential information from the message.

7. Carefully edit and proofread the e-mail message before hitting the "send" button. Don't let the immediacy or informality of using e-mail become a substitute for professional standards or attention to detail. Remember, don't put anything in an e-mail message that you would not want to see or hear in tomorrow's local or national news!
8. And above all, ensure the message does not contain inappropriate language, including language that is:
  - Obscene or racially motivated
  - Harassing or menacing
  - Negative or defamatory
  - Unsubstantiated opinion, rumor, or innuendos.<sup>3</sup>

### **Metadata: Information About the E-mail Message is Critical.**

Receiving an e-mail message that has missing information such as a subject line, a signature, or the full name of the sender can raise your skepticism about the legitimacy of that e-mail message. The same is true for e-mail messages created during the course of business — an agency or department must be able to demonstrate who originated a message and who controlled it at various times during its lifecycle.<sup>4</sup> An e-mail message without good metadata (or data that provides information about a certain item's content) can jeopardize the *authenticity* of the message, an important evidential consideration as well as an essential component for the long-term preservation of public records.

An e-mail message is authentic when it is proven that it is what it claims to be. Changes to the content of the message and/or missing information about the origins of the e-mail message can negatively affect authenticity and result in challenges to its accuracy and credibility.

It is recommended that the following metadata be included in every e-mail message created in the course of government business:

- When possible, the full name or address of the recipient(s) in the "To", "Cc", and "Bcc" fields, *not* shortened versions of the name(s)/address(es) or the name of distribution lists. A distribution list is a group of recipients that are referenced under a common name. For instance, if an employee is a member of an accounting committee, then a list can be created that contains the e-mail addresses of all of the members of that committee.

Example: Use "To: [fred.smith@xyzcorp](mailto:fred.smith@xyzcorp); [kim.jones@nc.gov](mailto:kim.jones@nc.gov); etc.", *not* [cancungirl@xyz.corp](mailto:cancungirl@xyz.corp); [Accounting Committee](#); etc.

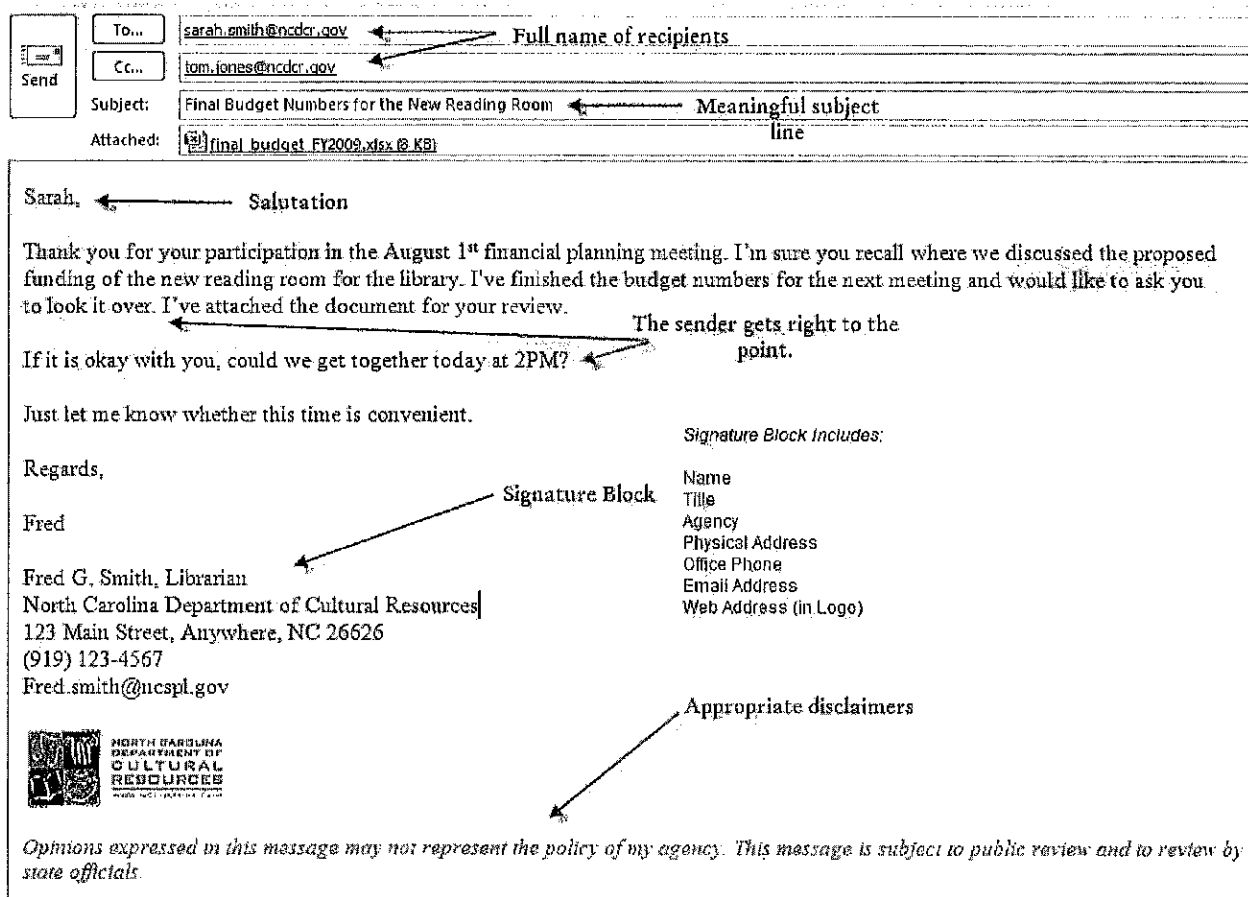
**Note:** *It is recommended that "Bcc" be used sparingly or not at all. Bcc details are stripped out by e-mail servers and this metadata is lost. We recommend contacting the person(s) directly if the information intended for the Bcc recipient(s) is confidential in nature.*

<sup>3</sup> Email Rules: A Business Guide to Managing Policies, Security, and Legal Issues: 36.

<sup>4</sup> Email Rules: 175.

- The full name or address of the sender in the "From:" field.
- A meaningful subject line. For example:
  - Instead of "Policy" use "Employment policy for your review"
  - Instead of "Question?" use "Question about new budget"
- The body of the message.
- All attachments with meaningful file names. See *Best Practices for File-Naming* ([http://www.records.ncdcr.gov/erecords/filenaming\\_20080508\\_final.pdf](http://www.records.ncdcr.gov/erecords/filenaming_20080508_final.pdf)) for more information.
- A signature block and the disclaimers as outlined in the E-mail Policy. The signature block should include information that makes the sender easily identifiable to the recipient(s).

The e-mail message in **Figure 1** is an example of a business message incorporating helpful metadata.



**Figure 1.** E-Mail Message Example

## Dealing with Threads.

You've probably seen e-mail threads lurking in your e-mail inbox. These are the "reply-all" messages that contain a series of replies back and forth pertaining to a certain message. These long messages often have countless senders and recipients and erratically inserted comments, making it nearly impossible to decipher the original message. If you find yourself as an initiator or participant of a thread discussion, here are a couple of things you can do to reduce the confusion:

- Only involve those in the e-mail discussion that are critical to the e-mail discussion. No one likes being the recipient of correspondence in which they have no interest.
- Resist hitting the "reply all" button. Wading through scores of responses and exchanges by people not only wastes time, but potentially overwhelms the e-mail system when too many of the recipients reply (often accidentally) to the entire list.
- Clearly identify new content from the original content. This can be done by entering replies or comments in a solid block, rather than inserting new content at various points in the original content<sup>5</sup> or by using different colored fonts to identify new content.
- And lastly, be consistent *where* the replied text or comment is inserted into the e-mail thread. Insert it either below or above the original and don't mix the two, as this makes it difficult to follow the thread of the message at a later date.

---

<sup>5</sup> DCC Digital Curation Manual: 32.

## Section 2 – Managing Your Inbox

---

### Managing E-Mail Messages

Managing e-mail messages should be a part of your daily routine. Making decisions about which e-mail messages to keep and which to discard will not only allow you to keep the size of your inbox manageable, but early retention and disposition decisions also help minimize the risk of misplaced, accidentally deleted, or misfiled e-mail messages.

#### What to Keep and What to Toss.

E-mail messages can have different versions (i.e., draft versus final), exist in multiple copies, and have a variety of attachments, so it is oftentimes challenging to decide what or what not to keep.

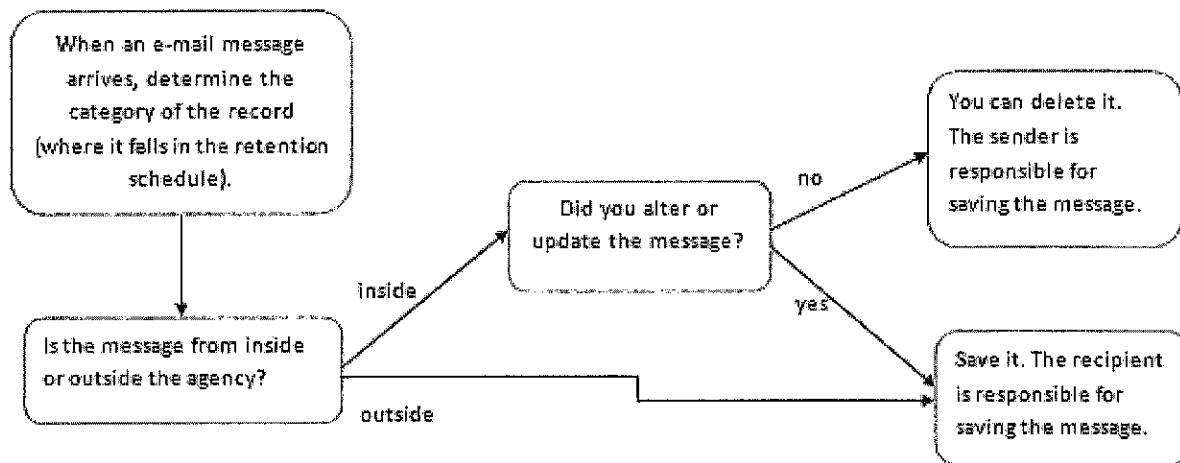
- *Drafts.* Unless there is a compelling reason, there is generally no reason to keep a preliminary draft of the e-mail message, provided the final version is retained and may be relied on as the official record. The same holds true for e-mail messages that contain successive drafts of documents.<sup>6</sup> Refer to the *Public Records with Short-Term Value* guidelines (<http://www.records.ncdcr.gov/guidelines.htm#short>) for further information about drafts and other short-term type records.
- *Copies.* Because e-mail messages can be sent and forwarded to multiple people, copies of the messages may exist in many areas of an agency. In most cases, the author, or creator, of the e-mail message is responsible for maintaining the "record" copy. However, cases in which the recipient has altered the message (made changes, added attachments, etc.), or when the message is coming from outside the agency (and therefore not documented anywhere within the agency); the recipient is the one responsible for retaining the message.<sup>7</sup> The decision tree in **Figure 2** on the next page will help guide you in this decision-making process.
- *Attachments.* Attachments are files, such as spreadsheets, documents, videos, or images that are affixed to the e-mail message. In many cases, the attached file is saved and managed somewhere other than in the e-mail application and the e-mail message is simply the carrier to send the file to someone else.
  - If you are the **owner/creator** sending an e-mail message with an attached file and you have already saved the file to a different location, only keep the e-mail message if it provides contextual or evidential value for the attached file.
  - The same guidelines apply if you are the **recipient** of an e-mail message with an attached file, provided you save the file to a different location. If you do not save the file, but alter the e-mail message (e.g., make suggestions) you are responsible for retaining both the e-mail and the attachment.

---

<sup>6</sup> Email Rules: 102.

<sup>7</sup> DCR Online Tutorial: Managing Your Inbox: E-mail as a Public Record  
([http://www.records.ncdcr.gov/tutorial\\_email\\_20080801/index.html](http://www.records.ncdcr.gov/tutorial_email_20080801/index.html))





**Figure 2.** Decision Tree. This graphic was borrowed from the Kentucky Department for Library and Archives "Guidelines for Managing E-mail in Kentucky Government," last updated September 5, 2005.

### Don't Forget Those "Sent" E-mail Messages!

When managing your inbox, it is quite easy to overlook or completely ignore those e-mail messages in the "Sent Items" folder. These e-mail messages need the same attention as those in your Inbox folder. If you receive an e-mail message and reply to it, you only need to keep the sent message. The original received e-mail message can be permanently deleted from your inbox.

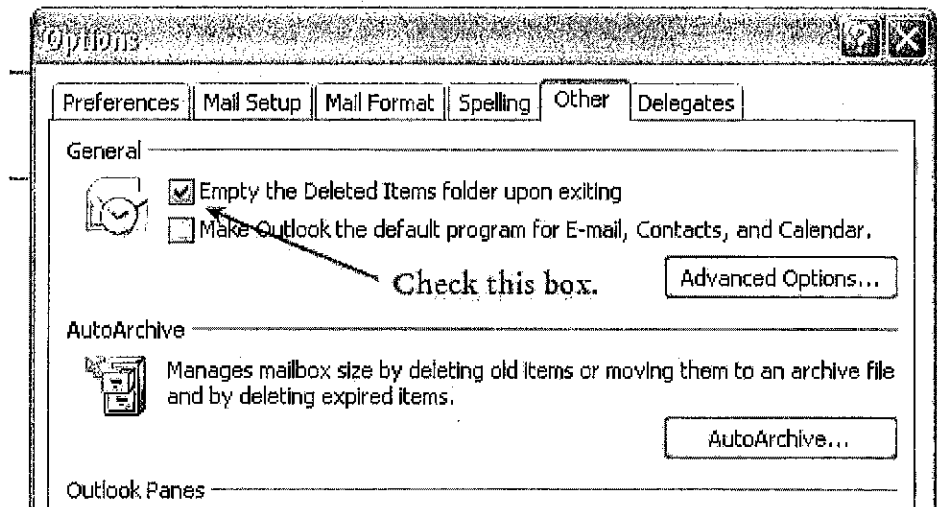
### Deleting E-Mail Messages. Are they really gone?

E-mail systems differ in their deletion functions. In Microsoft Outlook 2007, deleting an e-mail message sends it to the "Delete Items" folder, where it is held until you instruct the system to empty or purge messages that have been marked for deletion. So when you hit the 'delete' button, remember that the message isn't really deleted. Please note that public employees of Executive Branch agencies are subject to additional retention and disposition policies as outlined in Executive Order No. 18. Executive Branch employees shall not permanently delete any e-mail messages that they **send** for at least 24 hours, and shall not permanently delete any e-mail messages they **receive** for at least 24 hours except that they may immediately and permanently delete any e-mail messages they **receive** that are not clearly related to the transaction of State business, such as e-mails containing advertising materials or offensive materials. After 24 hours, Executive Branch employees shall retain or delete e-mails they have sent or received according to the retention schedules for their agency established by the Department of Cultural Resources.

There are two ways to permanently delete e-mail messages from your mailbox; automatically or manually:

- To automatically empty the 'Deleted Items' folder:

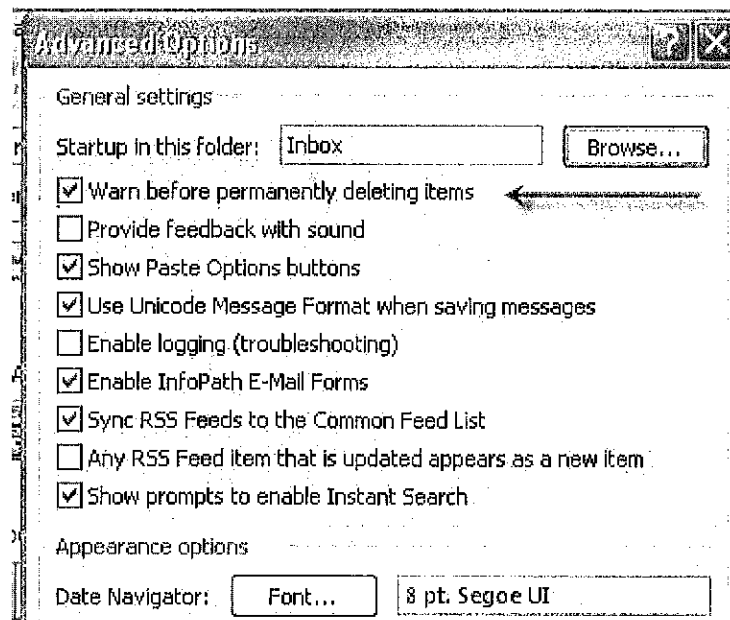
- On the navigation bar at the top of the screen, select **Tools**, click **Options**, and then click the **Other** tab.
- Select the **Empty the Deleted Items folder upon exiting** check box (see **Figures 3 and 4** on next page).



**Figure 3.** Delete items.

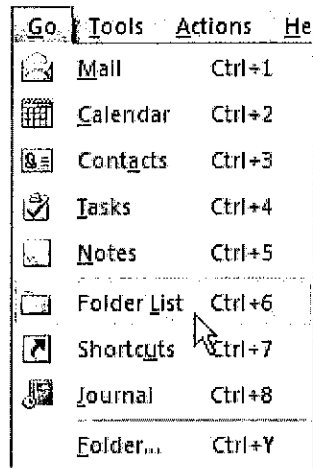
If you want to be notified (or “warned”) before the Deleted Items folder is emptied automatically, do the following:

- Click **Advanced Options**
- Clear the **Warn before permanently deleting items** check box.

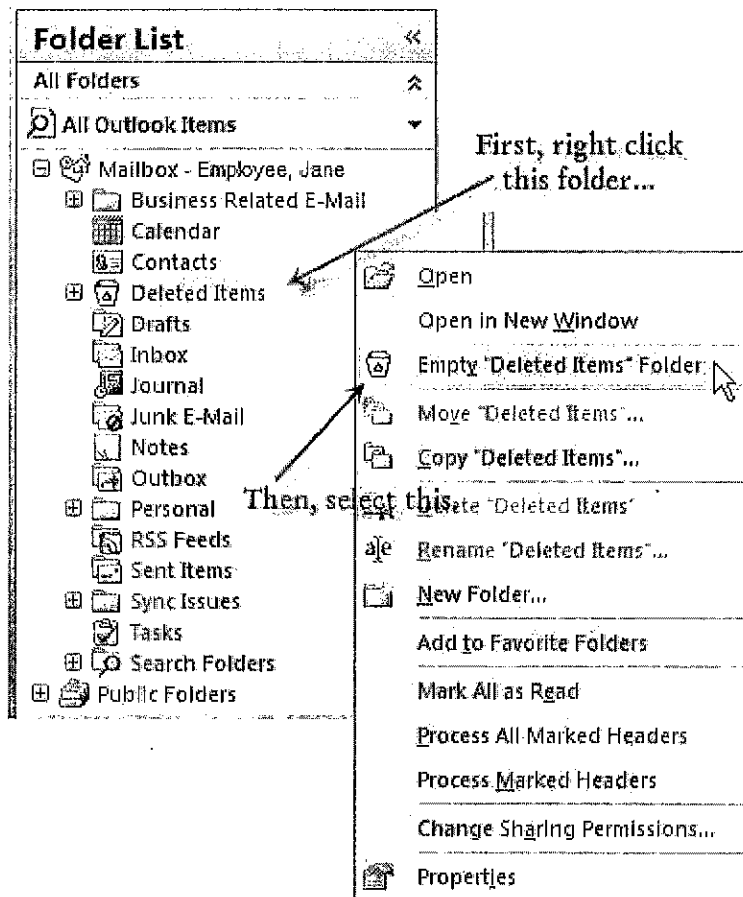


**Figure 4.** Advanced options.

- To manually empty the 'Deleted Items' folder:
  - On the navigation bar at the top of the screen, select **Go**, then click **Folder List**.



- In the **Folder List**, right-click the **Deleted Items** folder, and then on the shortcut menu, click **Empty "Deleted Items" Folder**.





It is important to know that currently e-mail messages are files stored on your computer's local/shared network or on a server. If e-mail messages are not deleted from your mailbox *before* ITS backs up the network/server to backup tapes, your e-mail messages still exist! Even after ITS deletes the information backed up on tapes, your e-mail messages still may not be permanently deleted — it sometimes takes 8 times to permanently erase (or overwrite) information from a back up tape. Please note that in accordance with EO 18, ITS will be procuring an e-mail archive system to be used for all agencies for which it provides e-mail services. E-mails will be retained in this system for 10 years. As such, this section will be updated as the e-mail system comes online.

The best advice is to use your email system wisely. Don't put something in e-mail that you do not want to be reviewed in the future.

## Section 2 – Managing Your Inbox

---

### Storing and Organizing E-Mail Messages

Due to the sheer volume of e-mail messages exchanged between users each day, e-mail boxes can quickly become unmanageable if proper storage and subsequent organization is not put into practice. A good filing structure not only makes it easy to search for specific e-mail messages, but also makes it easier to apply disposition instructions.

There are three ways to store retained e-mail messages:<sup>8</sup>

1. **Store the e-mail messages electronically.** If you choose to store messages in their original digital format you have two available options: keeping the messages in the e-mail client (in this case Microsoft Outlook 2007) or saving the messages to your network or hard drive.

#### Option 1 – Keeping the e-mail messages in the e-mail client

This option requires the least amount of effort as you don't have to move the messages out of Microsoft Outlook. It ensures quick access when your e-mail messages are well-organized and maintains the full functionality of the e-mail message, including preserving the metadata. This allows you to recall the message at any time for referencing and responding.

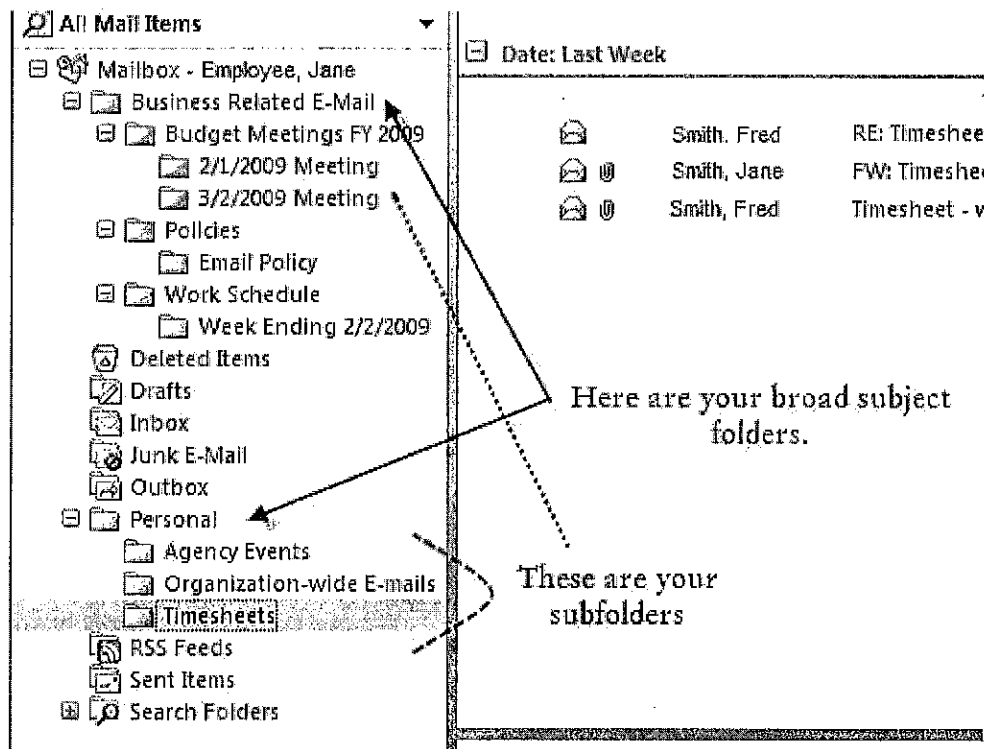
The easiest way to organize messages in your mailbox is to mirror the organization used in managing your other electronic documents. You can think of this type of organization as a tree – first create subject folders for broad categories, such as “Business E-mail” and “Personal E-mail” and then under these broad categories, create subfolders for narrower subjects such as “Budget Meetings” and “Agency Announcements.” The subjects, categories, and number of folders and subfolders is entirely up to you, but make sure that the folder title accurately describes the messages you will file there.

Once you have your folders set up, it is just a matter of moving the e-mail messages to the appropriate folders on a regular basis. **Figure 5** on the next page is one way to organize your mailbox.

For complete instructions on setting up folders in Microsoft Outlook 2007, see the Online Tutorial *Managing Your Inbox* at [http://www.records.ncdcr.gov/tutorial\\_email\\_20080801/index.html](http://www.records.ncdcr.gov/tutorial_email_20080801/index.html).

---

<sup>8</sup> Adapted from DCR Online Tutorial. [http://www.records.ncdcr.gov/tutorial\\_email\\_20080801/index.html](http://www.records.ncdcr.gov/tutorial_email_20080801/index.html) (accessed March 6, 2009).



**Figure 5.** Example of organization of e-mail mailbox.

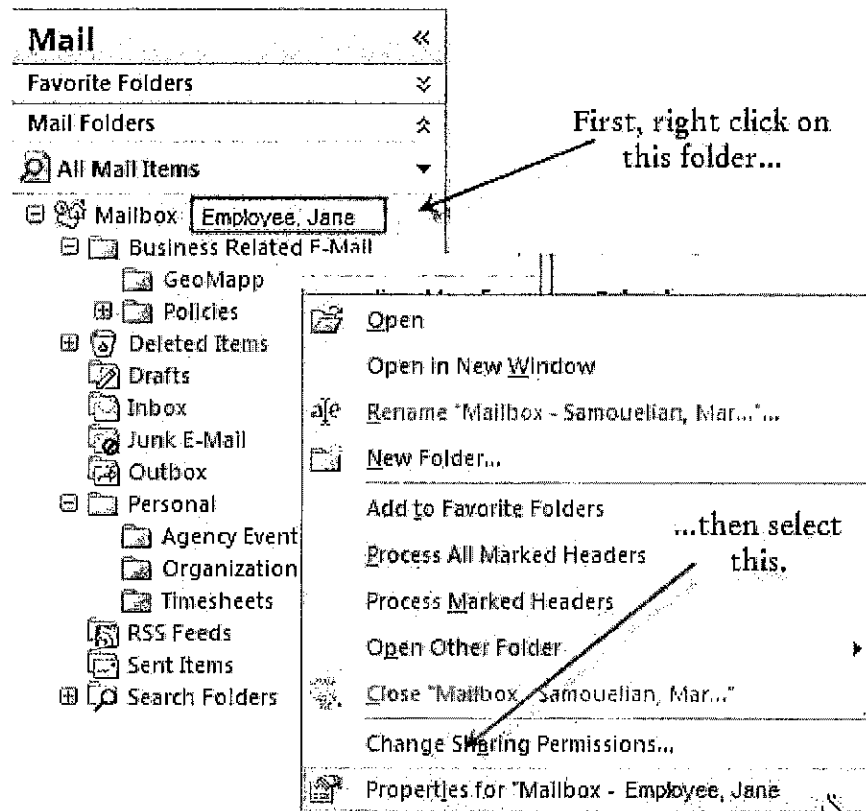


If you decide to store your e-mail messages electronically on the NCMail Microsoft Exchange server, it is important to understand that you either have 512 MB of storage (full service) or 30 MB of storage (basic service) available for e-mail messages depending on your agency's service agreement with ITS.<sup>9</sup> Your agency will be charged additional fees if you use more storage than these fixed amounts. To avoid these additional charges to your agency, you can back up these e-messages to your computer's network or hard drive or set up a personal folder (.pst) within Outlook that is stored outside of Exchange. Check with your IT department to determine your level of service.

<sup>9</sup> ITS Service Catalog. <http://www.its.state.nc.us/ServiceCatalog/eMailandCalendarServices.asp> (accessed March 6, 2009).

To determine the amount of storage you are using:

- Right click on the main **Mailbox** folder and select **Properties for Mailbox**.



- Click the **Folder Size** button at the bottom of the pop-up window.

General Home Page Permissions

Mailbox - Employee, Jane

Type: Folder containing Mail and Post Items

Location: Microsoft Office Outlook

Description:

☒ Show number of unread items  
☐ Show total number of items

When posting to this folder, use: IPM.Post

☒ Automatically generate Microsoft Exchange views

Folder Size... Advanced... Upgrade to Color Categories...

- This number is in kilobytes. To determine megabytes, divide by 1,024.

Folder Size

Local Data Server Data

Folder Name: Mailbox - Employee, Jane

Size (without subfolders): 0 KB

Total size (including subfolders): 2218 KB

Subfolder	Size	Total Size
Business Related E-Mail	0 KB	1440 KB
Business Related E-Mail\Geo...	350 KB	350 KB
Business Related E-Mail\Policies	0 KB	1091 KB
Business Related E-Mail\Polici...	1091 KB	1091 KB
Calendar	0 KB	0 KB
Contacts	0 KB	0 KB
Deleted Items	42 KB	42 KB
Deleted Items\Budget Meeti...	0 KB	0 KB
Deleted Items\Budget Meeti...	0 KB	0 KB
Deleted Items\Budget Meeti...	0 KB	0 KB

Close



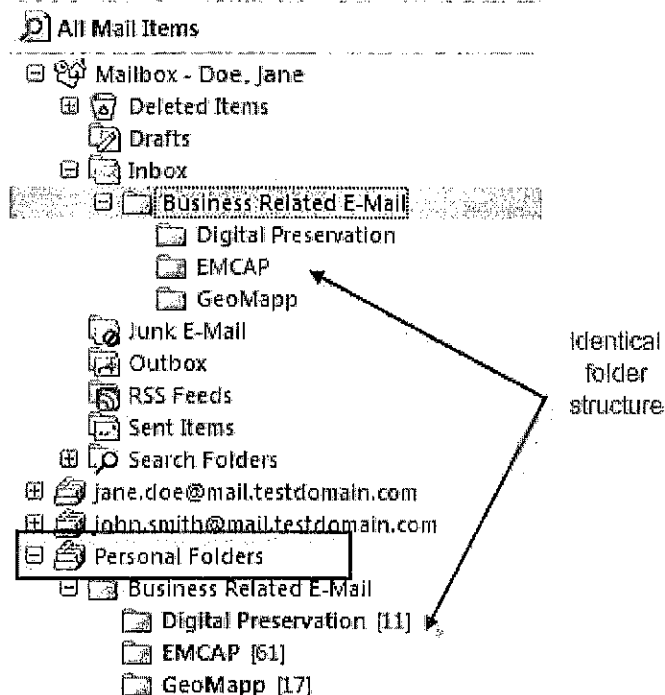
## Option 2 – Save the message to your network or hard drive.

Regularly backing up pertinent or important e-mail messages to your agency's network or to your computer's local hard drive is a good way to ensure that these messages are stored somewhere other than on the e-mail server. Backing up e-mail messages may be important: 1) if an issue arises with the NCMail Microsoft Exchange server and it is difficult to retrieve critical e-mail message(s) or they cannot be retrieved at all, 2) if your employment with the government is ending and your e-mail messages must be addressed and/or saved somewhere for a supervisor to view them before your computer can be "wiped" (data erased) and reassigned to another individual, or 3) if you need to free up storage space on the e-mail server because it is nearing your maximum storage usage.

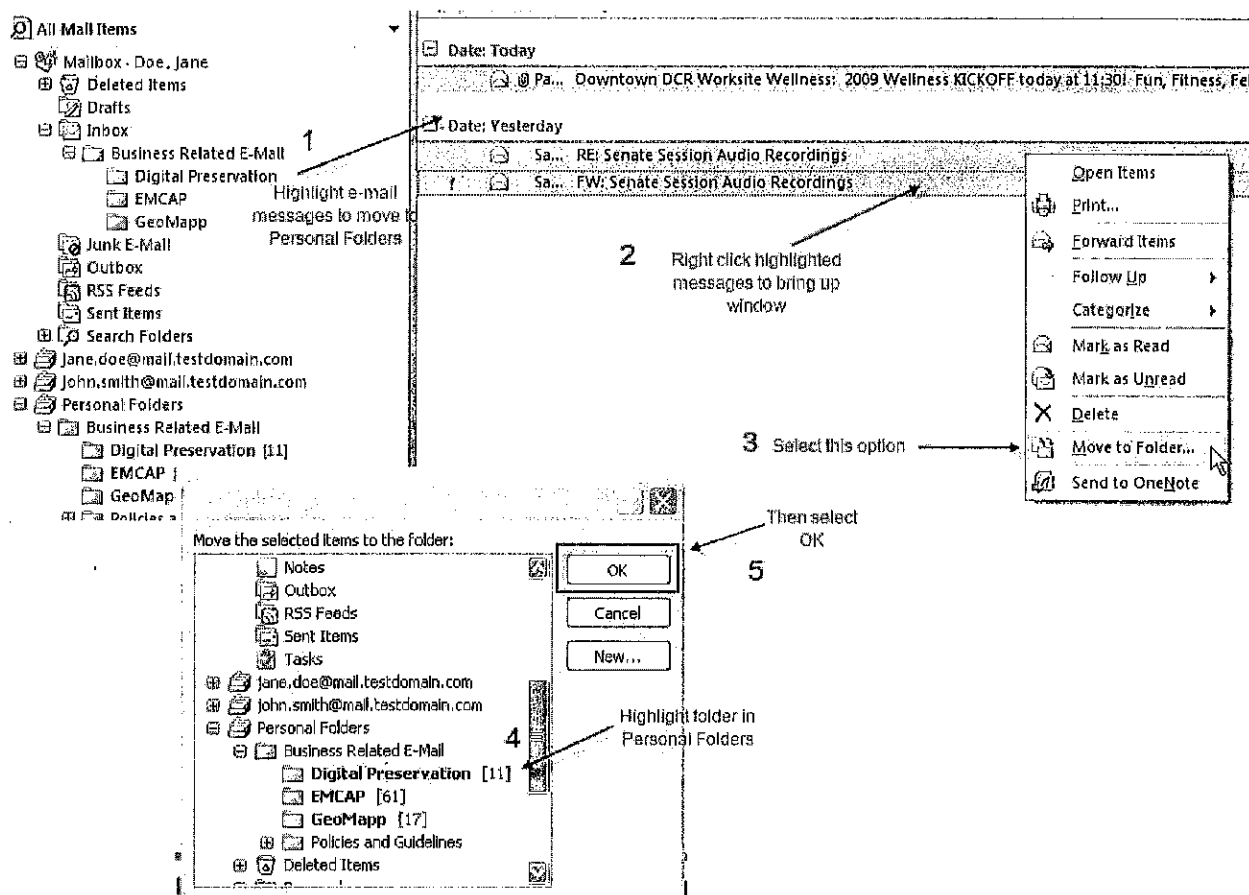
Microsoft Outlook stores e-mail messages in a data file known as a Personal Storage Table (.pst) which can be saved to the network or to your computer's hard drive. It is recommended you save e-mail messages as a .pst file when these messages need to be opened or accessed using Microsoft Outlook.

### To save your messages as a .pst file:

- **If Personal Folders folder already exists.** You may notice that a Personal Folders folder already exists in Outlook's default sidebar. When Outlook saves items to your computer's hard drive, it uses a type of data file called an Outlook Personal Folders file (.pst). Any messages that are moved to this folder are saved as a .pst data file. As this Personal Folders file is empty, you will first need to create subfolders to match the folders you previously created in your Mailbox Inbox (see steps on page 12). This will ensure easy movement between your inbox folders and the Personal Folders folder.

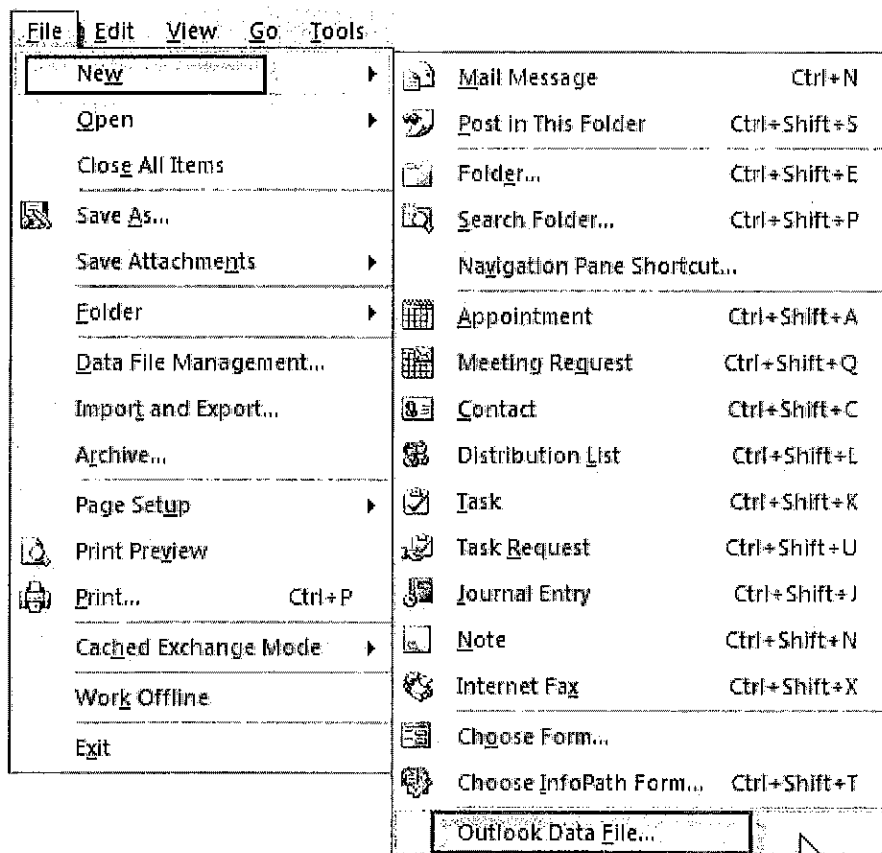


- To move your e-mail messages to the appropriate Personal Folders subfolder, highlight the e-mail messages in the Inbox folder, by holding down the **Ctrl** key and clicking the individual e-mail messages you would like to move.
- Right-click in the highlighted area. A new window will appear. Select **Move to Folder...**
- A Move Items window will appear. Highlight the destination folder in the Personal Folders and then select **OK**.

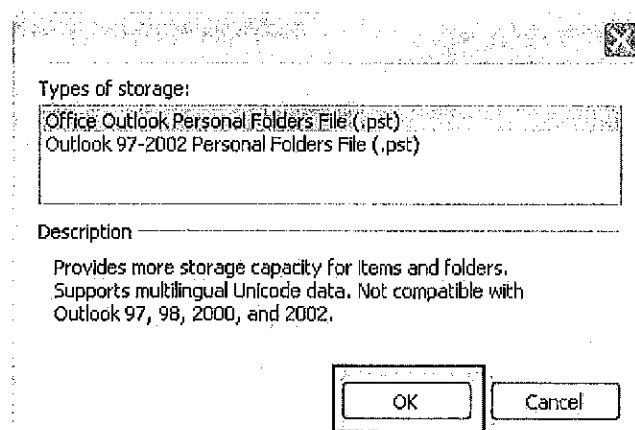


- You will note that these messages no longer exist in your Inbox folder. When you move a message to a new destination folder it deletes the message from the original folder.
- By default, Outlook data files are saved on your local drive at: *drive:* \Documents and Settings\user\Local Settings\Application Data\Microsoft\Outlook. If you navigate to this folder via Windows Explorer, you can view the size of the .pst file. The size will increase each time you move e-mail messages to the Personal Folders folder. If you need or want to store this .pst file on your agency's network or another location, see Appendix A for instructions.

- ***If a Personal Folders folder does NOT exist in Outlook's default sidebar.***  
Depending on how your computer was setup, you may not see a Personal Folders folder in Outlook. If this is the case, you will need to create one in order to move e-mail messages out of your mailbox Inbox and have them stored as a .pst file.
- Open the Microsoft Outlook e-mail client. From the toolbar, select **File → New → Outlook Data File.**



- A New Outlook Data File window will appear.



- "Office Outlook Personal Folders File (.pst)" will be highlighted. Unless you are certain that the outlook data files predate 2002, you can keep this selection highlighted and then select the **OK** button.
- Browse and select a location for the new .pst file in the Create or Open Outlook Data File window. This location should either be in a folder on your hard drive or in a folder on the network. Note that if your supervisor or IT needs access to your pst file, you will need to discuss where to save the pst file. Type in the new **Name** in the blank Name: field and then click **OK**.
- A Create Microsoft Personal Folders window will appear.

File: C:\Outlook pst Files\Test.pst

Name: Personal Folders

Format: Personal Folders File

Password: *These can be left blank*

Password: *These can be left blank*

Verify Password: *These can be left blank*

☐ Save this password in your password list

OK Cancel

- Type in the name of the folder you are creating in the **Name:** field (it is recommended you give the folder the same name as the newly created .pst file). The Password option should be left blank. Click **OK**.
- The new folder you just created will appear in the Outlook Mail tree on the left of the screen.
- Following the instructions beginning on page 16 for creating folders and moving e-mail messages.

***To save your messages in another file format:***

Saving messages to the network in another format, such as PDF, is a good idea when an e-mail message might be frequently needed by co-workers who do not have Microsoft Outlook to access the message. Saving it in another format means they can access it like any other file on your shared network.

For complete instructions on saving e-mail messages to another format, see the Online Tutorial 'Managing Your Inbox' at [http://www.records.ncdcr.gov/tutorial\\_email\\_20080801/index.html](http://www.records.ncdcr.gov/tutorial_email_20080801/index.html).

2. **Print the e-mail message and interfile.** You may opt to print the e-mail message and interfile it with other related public records. When printing an e-mail message, you should save all the metadata, including the sender, recipient, date and time sent, and the subject line. Printing using **File → Print** in Microsoft Outlook will ensure this information is included. Don't forget about the attachments!
3. **Print to microfilm.** Using technology resources available through the Department of Cultural Resources, your agency can print both electronic and paper records to microfilm. For more information, contact the Imaging Unit of Archives and Records (<http://www.records.ncdcr.gov/imaging.htm>)

### How Long Should These Messages be Stored?

The e-mail policy stresses that e-mail messages can have one of three different values depending on the content and function of the message to the agency. The value of the messages determines the length of time you should store them on your e-mail client. The matrix below is a rule of thumb for storage length. Remember though, that how long you keep an e-mail message is determined by your agency's retention and disposition schedule.

Please note that public employees of Executive Branch agencies are subject to additional retention and disposition policies as outlined in Executive Order No. 18. For Executive Branch employees, e-mails will be backed up for 10 years. The table below is a helpful guide for employees to manage their e-mail according to their records retention and disposition schedules.

	<b>Short-Term Records</b>	<b>Long-Term Records</b>	<b>Permanent Records</b>
<b>Retention</b>	Typically less than 5 years	Typically more than 5 years, but less than 10.	Typically more than 10 years. Depending on value, could be kept indefinitely.
<b>Length of Storage</b>	Store on e-mail client until it out serves its purpose.	Shouldn't remain on e-mail client for more than a year, preferably six months.	Store on e-mail client until a permanent copy or microfilm can be made.
<b>Action</b>	Permanently delete e-mail message from e-mail client after it serves its purpose.	Save on network or transfer to another storage medium such as a CD or DVD. After successful transfer, original e-mail message can be permanently deleted from e-mail client.	Once permanent copy or microfilm, original e-mail message can be deleted from e-mail client.

### Organization and Storage Options Using Microsoft Outlook.

As all state government employees are moving to Microsoft Outlook, there are some optional tools for assisting you in organizing and storing your e-mail messages in Outlook. *Care needs to be taken in setting up these tools to ensure they are in agreement with your agency's retention and disposition schedule.* We recommend first trying out a feature or two in each tool — to

make sure they do what you want them to do — before implementing them to fully manage your e-mail messages.

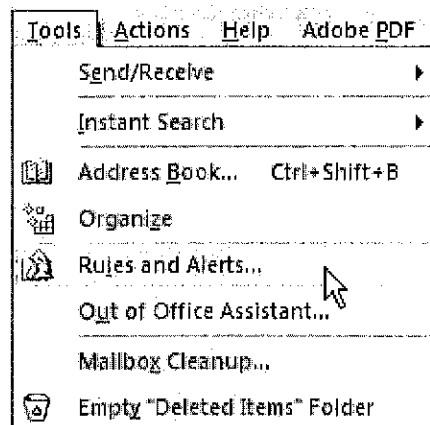
- The **Rules and Alerts** option in Outlook can help you manage your e-mail messages by performing actions on messages that match a specific set of conditions (or rules). After you create a rule, Microsoft Outlook applies the rule when a message arrives in your **Inbox** or when you send a message\*.

*\* Employees subject to EO 150 cannot use the rules function.*

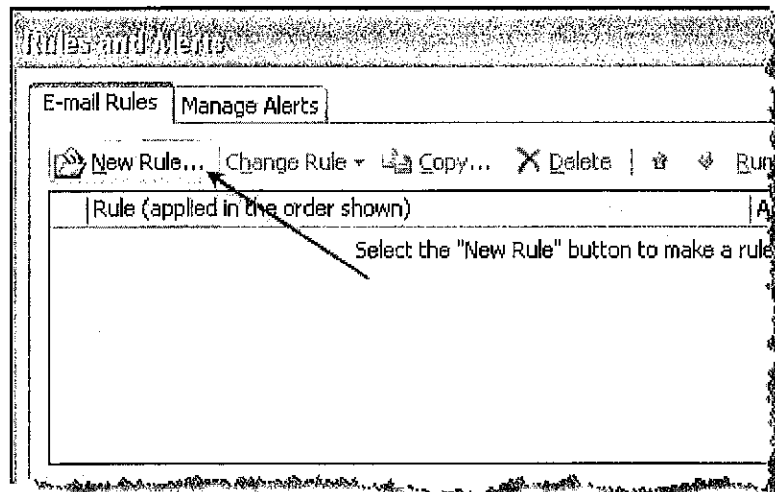
Rules fall into two general categories: notification and organization. Notification rules alert you in some way when you receive a particular message. Organization rules perform one or more actions on a message. For example, you can create a rule that moves certain messages to a folder that will later be deleted as prescribed by a retention schedule.

Rules can be created using either a template or from scratch.

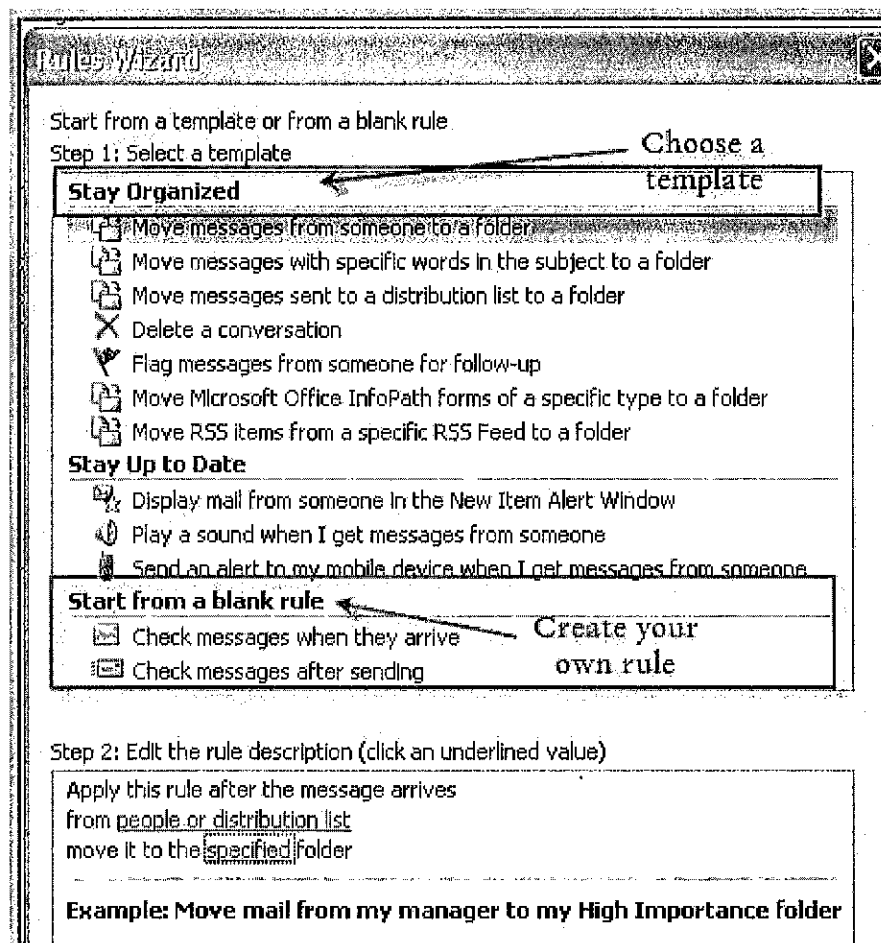
- To open Rules and Alerts, on the navigation bar at the top of the screen select **Tools → Rules and Alerts**.



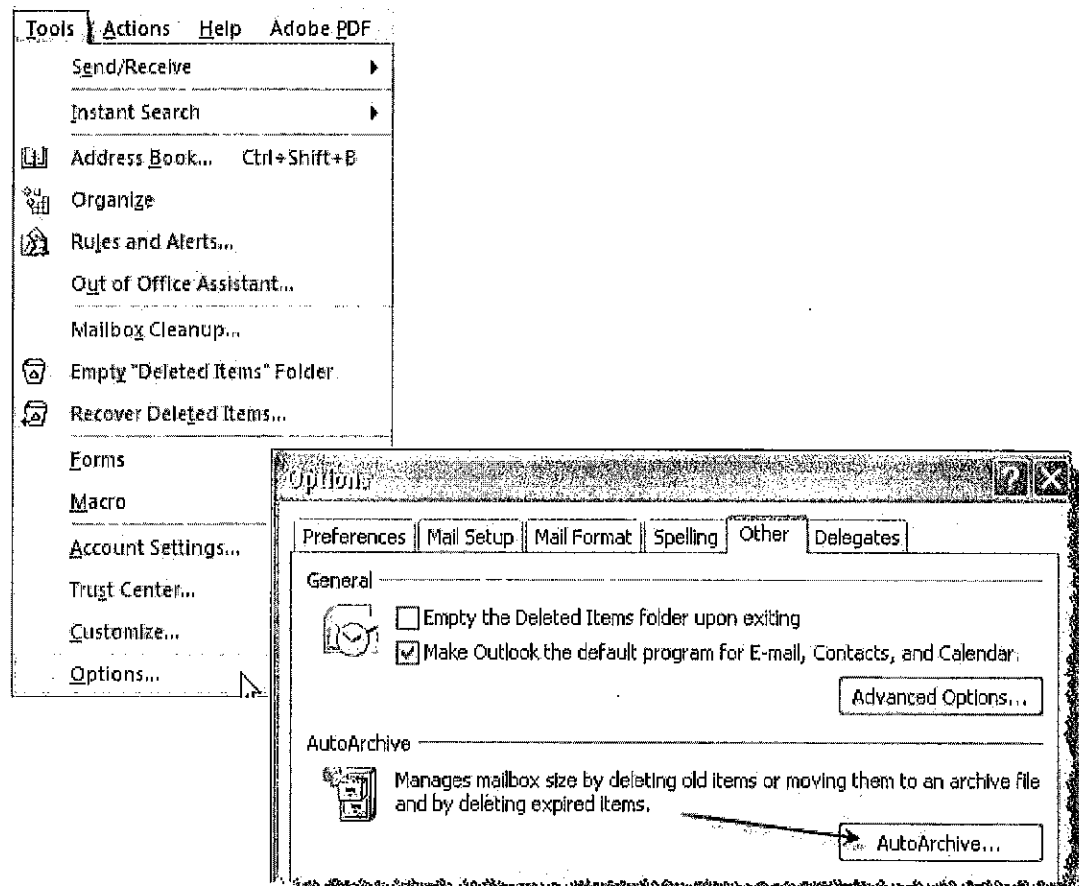
- A Rules and Alert pop-up window will appear. Select the **New Rule** button.



- From the **Rules Wizard** pop-up window you can either select a rule from a template or create a blank rule where you set the parameters.

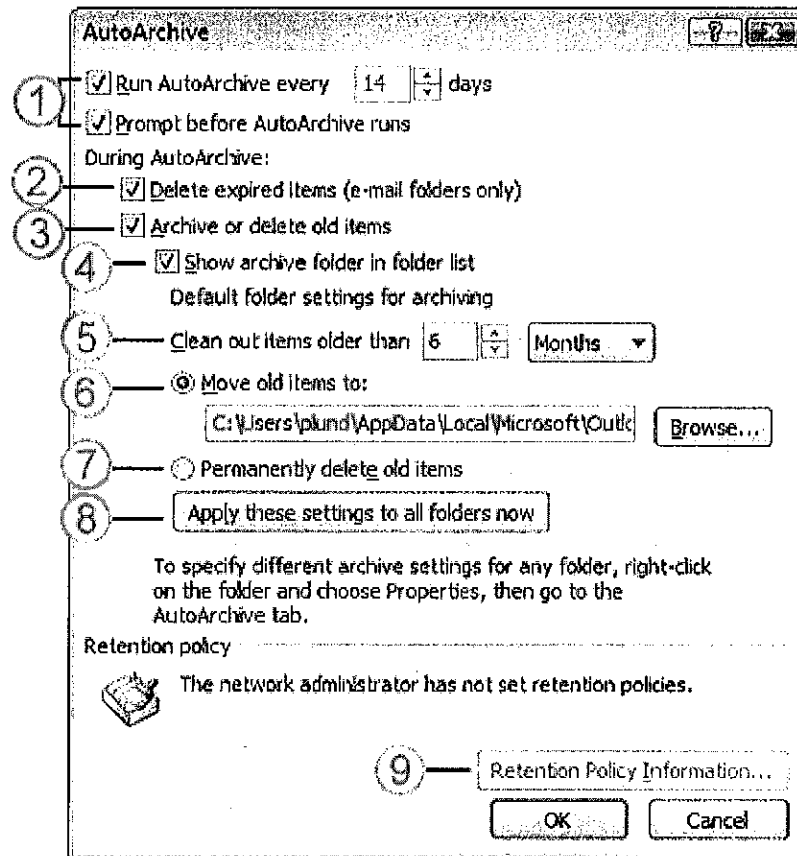


- As there are countless rule variations offered through this tool, it is not possible to show them all in this document. Choosing either the template **Stay Organized** or **Start from a blank rule** option will initiate a step-by-step process that will guide you in setting up rules that work best for you. From the Rules and Alerts window, you also have options to change rules, delete rules, or modify how often you want the rules run (periodically versus all the time). For additional information on rules and alerts, type in "rules and alerts" in the Outlook help box located at the right top of the screen and then press enter.
- The **AutoArchive** tool in Outlook has tools to help manage mailbox size by automatically or manually moving messages from their original location to an archive folder.
- To open AutoArchive, on the navigation bar at the top of the screen select **Tools → Options → Other**. Select the **AutoArchive** Button





- The AutoArchive screen is where you can set up the features that best suit your needs. See below for a description of each feature.<sup>10</sup> To ensure that pertinent e-mail messages are not accidentally deleted, moved, or misplaced, it is recommended that you are prompted before AutoArchive is run and that you **do not** automatically delete expired or old items.



**1 Run AutoArchive.** Choose how often you want AutoArchive to run. You should consider how many items you typically receive during a given time and adjust the timeframe accordingly. We strongly recommend you manually start the autoarchive process rather than have it run automatically as it could create a management nightmare. When you autoarchive, the computer assigns it a name that is not descriptive or logical, thus making it very difficult to find it again.

**Prompt before AutoArchive runs.** Choose this option if you want Outlook to display a reminder message before AutoArchive processes your Outlook items. When you see the message, you can click **No** to cancel that AutoArchive session (*note: this option is recommended*).

**2 Delete expired items (e-mail folders only).** This option is not selected by default. You can choose to have e-mail messages deleted when their aging period has expired. The default period for your Inbox and Draft items is six

<sup>10</sup> Adapted from Microsoft Outlook Help.

months and three months for your Sent Items, but you can change these periods using the **Clean out items older than** option (*note: this is not recommended*).

**3 Archive or delete old items.** Choose this option if you want your Outlook items archived, and then deleted when they reach the end of the aging period. Choose additional settings to apply to both archiving and deletion.

**4 Show archive folder in folder list.** Choose to have the Archive folder listed with your other working folders in the Navigation Pane. In the main **Archive** folder, you can open the subfolders and view your archived items. When viewing your archived items, you can verify that the correct items were archived, and you can also drag any items that you need back to a working folder.

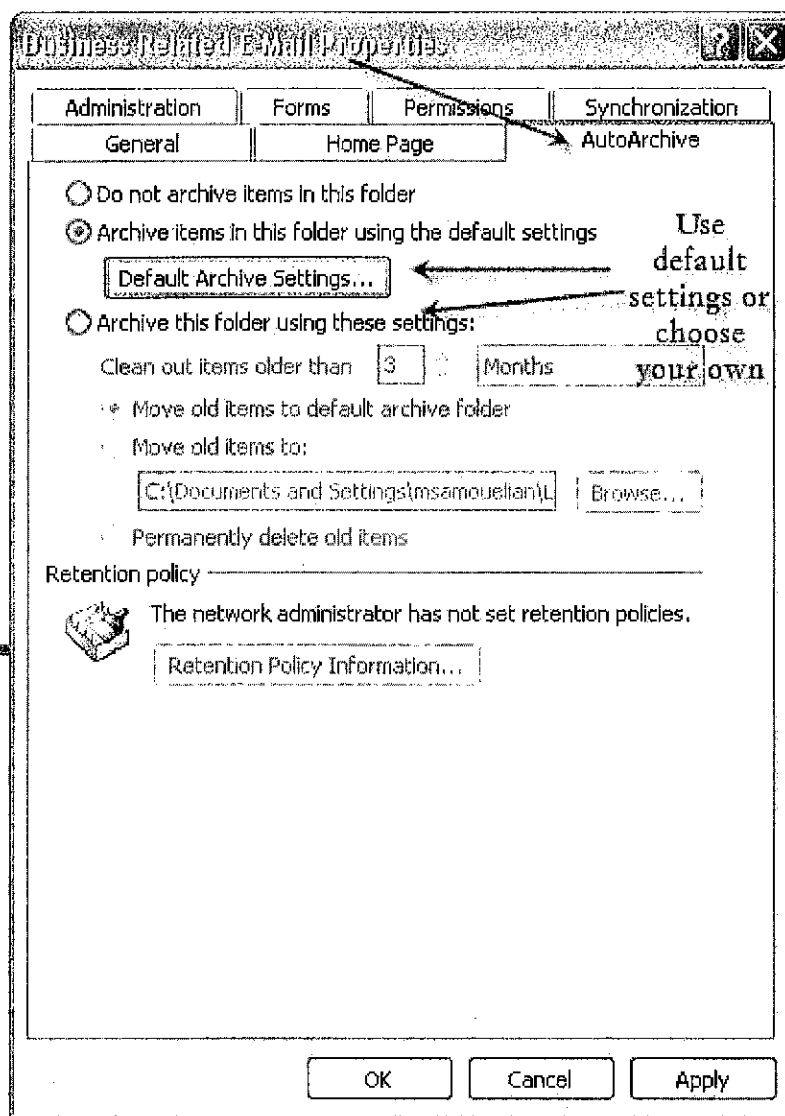
**5 Clean out items older than \_\_\_\_ time.** Choose the default configure for which items you want archived based on how old they are. You can configure a period of one day up to a period of 60 months. "Clean" means to archive — store — items. It does not mean "delete" unless you have selected that setting for the folders elsewhere.

**6 Move old items to.** The default setting for this location is different for computers running the Windows Vista and Microsoft Windows XP operating systems. If you want to set another destination for the archived items, you can browse to and set a different location. Items are moved to this location after their aging period.

**NOTE:** Items archived in a custom location are not deleted unless you open the folders and delete them manually.

**7 Permanently delete items.** This option immediately deletes the expired items instead of moving them to the default location, such as another folder that you designated or the Deleted Items folder (*note: this is not recommended*).

**8 Apply these settings to all folders now.** This option applies the AutoArchive settings, including your changes, to all of your folders. To specify different settings for one or more folders, do not choose this option. Instead, right click on any folder and choose **Properties**. Then go to the AutoArchive tab and select which settings will best fit your needs, and then select the **Apply** button. Note that changes made to specific folders apply only to those folders.



- For additional information on AutoArchive, type the term "autoarchive" in the Outlook help box located at the right top of the screen. Press **enter**.

## Section 2 – Managing Your Inbox

---

### Preserving E-Mail Messages

**File formats are a challenge for long-term preservation.**

We've all been in situations where the document you want to view just won't open. After trying several times, you come to realize that it's in a format that doesn't exist anymore (remember Word Star?). The same holds true for e-mail messages as most e-mail applications are not designed for long-term records storage.

The challenge of preserving e-mail messages for future access becomes greater if the format in which the messages are written is proprietary (meaning supported by just one type of software like Microsoft). Therefore, it is recommended that you convert e-mail messages with long-term value to an open, widely accepted (or non-proprietary) format. These formats include:

- **Rich Text Format (RTF)**, which can be opened in many word-processing software programs.
- **American Standard Code for Information Interchange (ASCII)**, identifiable by a .txt extension. ASCII is a plain-text format that, like RTF, is software-independent. However, ASCII is *literally* plain—meaning the representation of special formatting instructions (e.g., italics or bold type and hyperlinks) and the document structure (like indenting, spaces, and paragraphs) are lost when converted to ASCII.
- **Hypertext Markup Language (HTML) or Extensible Markup Language (XML)**. These are file formats that contain embedded instructions for displaying the content of the document. All header information, including server path, is converted and retained in the document. These files will open in a Web browser.
- **Portable Document Format (PDF)** is a file format created by Adobe Systems. It is used for representing documents in a manner independent of the application software, hardware, and operating system. An e-mail message saved as PDF most closely resembles the look of the original e-mail message and preserves all hyperlinks, however, it does not convert all of the header information including the server path.



It is important to remember when converting e-mail messages (regardless of format); any associated attachments *are not converted with the message*. Therefore, you must convert any attachments separately.

**To convert e-mail messages to RTF, ASCII (Text Only), or HTML** using Microsoft Outlook:

1. Click on the e-mail message (or messages) you would like to convert. To select multiple messages, hold the **Ctrl** key, and click the messages you would like to convert.
2. Select **File → Save As**. A new "Save As" window will appear.
3. Select the folder where you want to save the e-mail message.

4. If you are satisfied with the **File Name**, you can leave it as is OR you can type in a new file name.
5. From the **Save as type**: drop down list, select the format you would like to convert the e-mail message to (Rich Text Format [RTF], HTML, or Text Only [ASCII]), and then click the **Save** button.

**Note:** *not all file formats will be available for conversion. The format of the original e-mail message will determine which formats in Microsoft Outlook are available for conversion.*

To **convert e-mail messages to PDF** using Microsoft Outlook\*:

1. On the tool bar at the top of the screen, select **Adobe PDF** → **Convert to Adobe PDF** → **Selected Messages**.
2. Choosing 'Selected Messages' will convert individual messages. If you choose 'Selected Folders' all the messages in the folder will be converted to PDF.
3. A new "Save Adobe PDF As" window will appear.
4. Select the folder where you want to save the e-mail message(s).
5. If you are satisfied with the **File Name**, you can leave it as is OR you can type in a new file name.
6. Click the **Save** button.

*\*Conversion to a PDF format is only available to those users who have a full copy of the Adobe Systems tool OR Windows 2007 installed on their computer. For Windows 2007 users, a "Save as PDF or XPS" add-in application will need to be installed to give you the ability to convert messages to PDF. Contact your IT department for assistance in the installation of this add-in.*

Information technology staff may have to assist with converting large quantities of e-mail messages to one of these formats. These file formats may work well for the textual documents that are often attached to e-mail messages, such as word processing documents or spreadsheets. In cases where attachments are complex files such as computer-aided drawings or databases, it may be advisable to retain them in their original format, along with the software and operating systems required to access them; thus, preserving the structure of the records.

**The media on which e-mail messages are stored is fragile and not ideally suited for long-term preservation.**

Agencies that retain e-mail messages must provide a suitable storage environment and proper care and handling procedures. It is recommended that agencies research life expectancy estimates for storage media, develop systems to check the content of the media periodically, and convert to new media when necessary. You should plan on migrating your data to new storage technologies every 3-5 years. Refrain from using the least expensive CDs or DVDs as they are more susceptible to media rot than the slightly more expensive gold CDs and DVDs. For more information, please consult the *Protect Your DVDs and CDs* document at <http://www.records.ncdcr.gov/erecords/DVDCDhandling.pdf>.

The practice of storing e-mail messages with long-term value on machine-readable media such as CD-ROM, magnetic tapes, or microfilm presumes that the hardware and software required to read the data will exist into the future. Because commonly used media can be counted on to change as accepted technologies change, and as systems adapt to using standardized hardware, please contact DCR for information concerning currently acceptable media.

### Section 3 – Appropriate Use of E-Mail

---

It cannot be overemphasized that an e-mail message is considered to be a **public record** when created or received in the course of carrying out normal business activities. Once you send an e-mail message, you no longer have control over who might see that message or how it will be used. Messages sent quickly and in some cases thoughtlessly can result in hurt feelings, misunderstandings, and in the worst case scenario — liabilities. Adherence to basic rules including the best way to forward e-mail messages and guidelines for e-mail 'netiquette' can alleviate potential problems and help cast you and your agency in the best light.

#### **Think before you forward.<sup>11</sup>**

You might ask "what's the harm in forwarding an e-mail to my co-worker?" Disclosure of confidential or private information may occur when e-mail messages are forwarded to unauthorized users, directed to the wrong recipient, or printed in a common area where others can read them. Additionally, some of the latest e-mail scams that instruct you to forward an e-mail are intended to do more than just deceive you. Take extra care when forwarding messages. Make sure that you do not:

- Knowingly send out an e-mail message that contains viruses, Trojan horses, or other malware.
- Use the electronic-mail system or network resources to propagate chain letters, misinformation, or hoax information.
- Forward any confidential information to any unauthorized party without the prior approval of a local department manager.
- Forward the wrong attachment.
- Send information or files that can cause damage to the State of North Carolina or its citizens.
- Send large files (over one [1] megabyte) to individuals, as these files may have an undesired effect on the response and stability of the electronic-mail system.
- Send unsolicited messages to large groups of people except as required to conduct agency business.

#### **Minding Your Electronic 'P's and Q's'.**

The phrase "watch your p's and q's" has long been in use to encourage people to speak politely or to "mind their manners." The same etiquette holds true for composing and sending e-mail messages. Below are some basic guidelines for acceptable and effective correspondence.<sup>12</sup>

---

<sup>11</sup> Adapted from the State Security Manual – Chapter 3, Standard 030311.

<sup>12</sup> Adapted from Email Rules: 39-44.

- Don't use e-mail to let off steam. If you're upset or angry, compose yourself before typing your message. Once you hit that "send" button, your e-mail message is on its way through the e-mail system and likely can't be retrieved.
- Control the urge to "flame." An e-mail flame is one that is blunt, rude, insensitive, or obscene. Flames have no place in a business environment.
- Do not mail to the world. Send e-mail messages only to those individuals with a legitimate need for your information. If you send an e-mail message to thousands (or tens of thousands) of coworkers, not only is this a time waster for recipients, but the resulting traffic might cause the e-mail system to shut down and business to be interrupted.
- Don't use ALL CAPITALS or too many exclamation points!!!! It is the equivalent of shouting in the sphere of e-mail communication.
- Respect others' time. E-mailboxes filled with jokes, advertisements, recipes, and requests for charitable donations not only violate the E-mail policy, but also drain employee productivity and waste bandwidth.
- Consider e-mail's limitations. E-mail may be the best way to deliver news fast, but it's not necessarily the best route to a quick reply. Your recipient is under no obligation to check incoming messages, if at all. If you have a pressing issue, you may receive a faster reply by picking up the phone.

### **What is Persistence and Why Should I Care?**

Once you send an e-mail message, you lose control over that message and how it will be used. Even if you properly manage that public record according to your retention schedule, you cannot be certain that the recipient will do the same.<sup>13</sup>

For example, you send an e-mail to a colleague with a comment about another co-worker. You delete that e-mail from your sent box since it is not work-related. However, perhaps your colleague replies to your personal e-mail with information about a project you two are working on. Not only do you now have a public record that includes personal correspondence sitting in your inbox, your colleague has your original e-mail in her inbox, as well as a message that is a public record in her sent box.

Following the guidelines above will help to ensure this does not happen to you!

---

<sup>13</sup> DCR Online Tutorial.

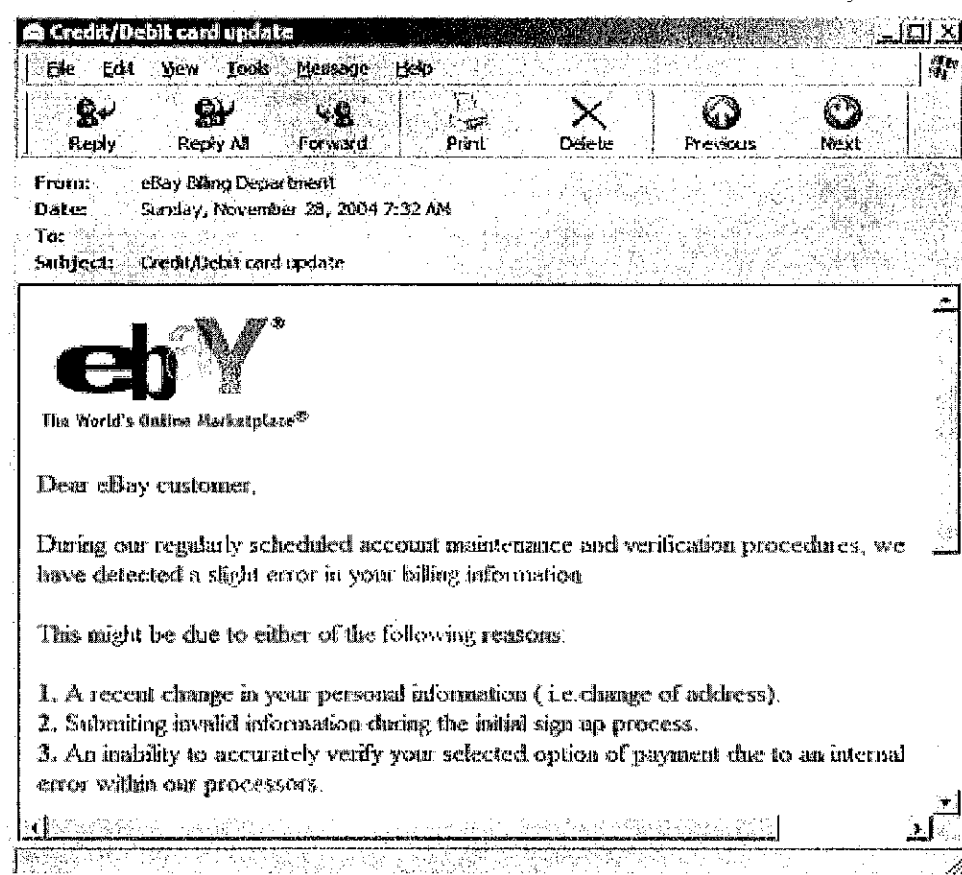


## Section 4 – Technical Security

The usefulness of e-mail is threatened daily by the increasing number of e-mail scams, spamming, and e-mail viruses. While ITS takes appropriate security measures to detect security breaches and other violations of system integrity, individual users must take all reasonable precautions to ensure the security of their *own* e-mail account. The primary means to do this is to first understand the possible threats to security and then learn what you can do to protect yourself from them.

- Almost as soon as e-mail became widely used, it began to be used to defraud people via **e-mail scams**. **Phishing** is perhaps one of more common scams.

Phishing occurs when the attacker sends an e-mail message purporting to be from a valid financial or eCommerce provider. The message often uses fear tactics in an effort to entice the intended victim into visiting a fraudulent Web site. Once on the Web site, which generally looks and feels much like a valid site, the victim is instructed to enter sensitive financial information such as their bank PIN number and their Social Security number. This information is then secretly sent to the attacker who then uses it to engage in credit card and bank fraud or identity theft. Here is an example of the e-Bay phishing scam:<sup>14</sup>



<sup>14</sup> "Watch Out for 'Phishing' Emails. <http://antivirus.about.com/od/emailscams/ss/phishing.htm> (accessed February 28, 2009).

*How to protect yourself from e-mail scams:*

- Banks, credit card companies, and financial businesses will NEVER ask for personal information in an e-mail message, and ITS will never ask for your password via an e-mail message. Legitimate messages and Web sites provide ways to contact the author or business directly.
- Don't be fooled by official-looking messages from state agencies, particularly ITS Messaging Services, which threaten to suspend your account(s).
- Follow your gut instinct. If it sounds too good to be true; it probably is.
- Be extra suspicious and vigilant. If you receive an e-mail message from someone you know but you aren't quite sure it's legitimate, compose a new e-mail message to that person or business and ask if they sent you a message. Don't reply using the message you received - the From address just might be bogus.
- Be aware that e-mail scams are a real threat to e-mail system security. If the sender's address isn't a person you know or is disguised generically, if there are obvious misspellings in the text of the e-mail, or if a link isn't displayed or the link points to an executable file, then the e-mail message is likely a scam.
- Guard your business e-mail address particularly when sending and receiving e-mails outside of the NCMail e-mail system. Consider having a separate, disposable e-mail account used only for registration and other online activities.
- Everyone receives e-mail messages that may pose personal or departmental risks. These types of messages, such as phishing messages, should be deleted from the e-mail system as soon as possible and according to law.
- **Spamming** is unsolicited commercial (or bulk) e-mail messages. Because of the very low cost of sending e-mail, spammers can send hundreds of millions of e-mail messages each day over an inexpensive Internet connection. Hundreds of active spammers sending this volume of mail results in information overload for many computer users who receive voluminous unsolicited e-mail messages each day.

*How to protect yourself from spam:*

- Spammers utilize a variety of sources to collect e-mail addresses; they find them on other Web sites, chat rooms, and newsgroups. So avoid using your business e-mail address to register or sign-up for accounts online. Consider having a separate, disposable e-mail account used only for registration and other online activities.
- Know who you're dealing with. Don't open or forward an e-mail message from an unknown sender.
- Knowing security is looking for specific headers, spammers will intentionally misspell words (e.g., "loose 30 ponds in 7 days"). Keep an eye out for these misspellings.

- Don't click on any links in a spam e-mail message, especially that 'unsubscribe' link – it only tells the spammer you're still there.
- Don't reply to spam or e-mail the spammer and ask to remove your address from his/her mailing list. This will only serve to confirm your e-mail address and encourage the sender to forward or sell it to other spammers.
- Recognize the common spam words or subject categories that appear in a subject line. These include Pornography, Money Making, Direct Products, Become a Spammer, Gambling/Sweepstakes, and Health Cures/Weight Loss.
- Be sure to report spam to your IT department. If your agency uses NCMAIL, you can report spam by copying the entire contents of the e-mail into a new e-mail message and sending it to spam@ncmail.net.
- Government agencies are often targets for **viruses**. An e-mail virus is a computer code or program designed to create mischief, intrude, exploit, or harm the computer environments used by and within most organizations.<sup>16</sup> Viruses typically enter computers through e-mail attachments. When the attachment is opened, the virus is executed and gains access to the network. Use the same guidelines as outlined above when protecting yourself from viruses. But in addition:
  - To succeed, viruses usually require executable programs. ITS makes every effort to block .exe files and many other harmful file types (for a complete list, see: <https://www.ncmail.net/blockedfiles.htm>). However, should you receive an executable program or attachment you do not recognize, look for clues that a virus may be present. If you have any doubt, don't open the attachment. If you are unsure of an attachment, contact your IT helpdesk – they can try to determine if it's legitimate.
  - Avoid opening any e-mail messages with subject lines you don't recognize or that simply don't make any sense (for example "Subject: I Love You" or "This is a great recipe!"). If you have any doubt, contact your IT helpdesk.

---

<sup>16</sup> Email Rules: 164.

## Contact Information for Government Records

For more information, please contact us at:

Department of Cultural Resources

Division of Historical Resources

Archives and Records Section

Government Records Branch

**Physical Location:** 215 N. Blount Street, Raleigh, N.C.

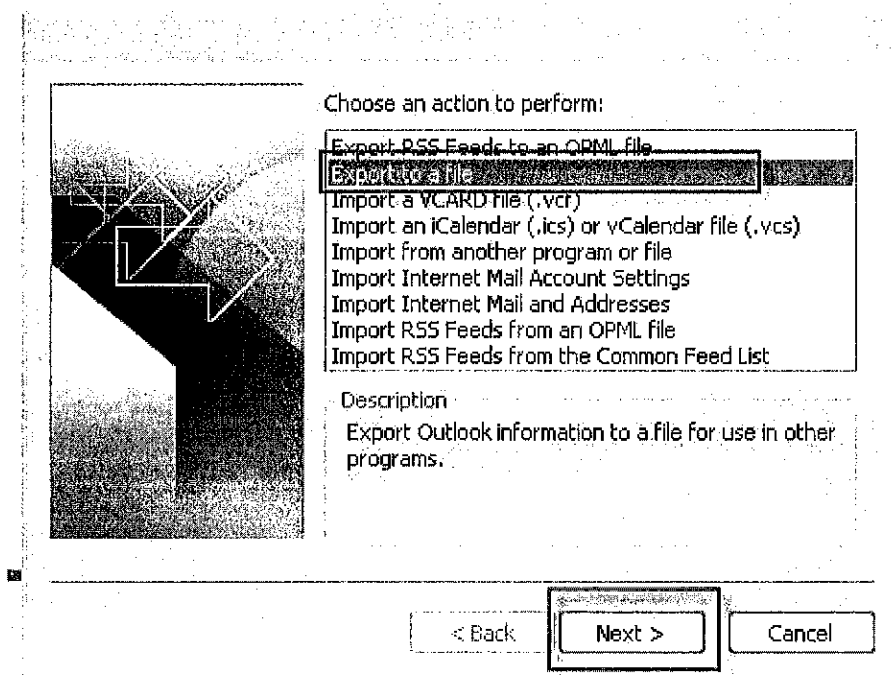
**Main Telephone:** 919-807-7350

**E-mail:** [Records@ncdcr.gov](mailto:Records@ncdcr.gov)

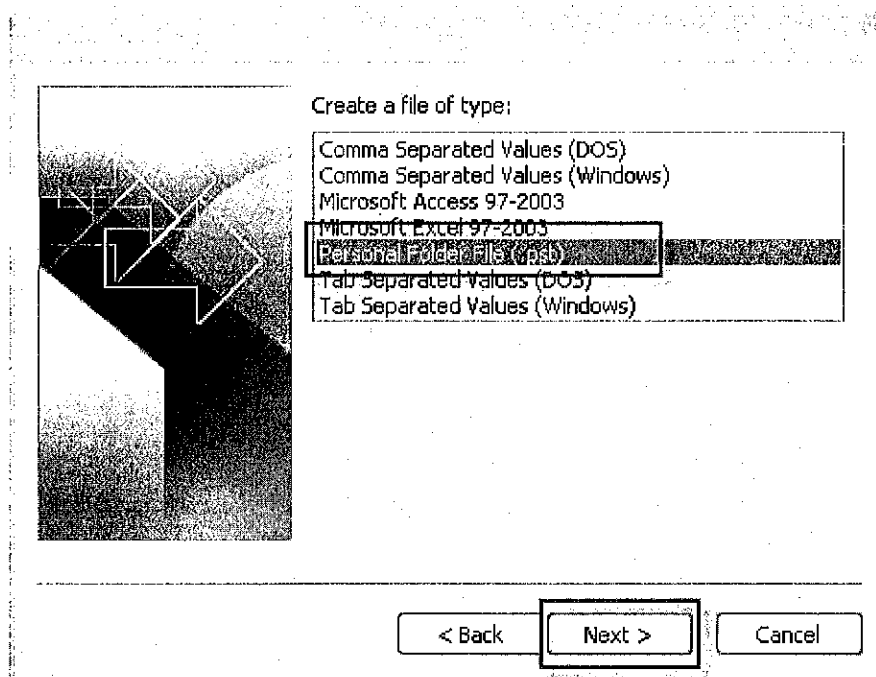
Or visit our **Web site** at <http://www.records.ncdcr.gov/default.htm>.

## Appendix A – Exporting Your .pst File to Another Location

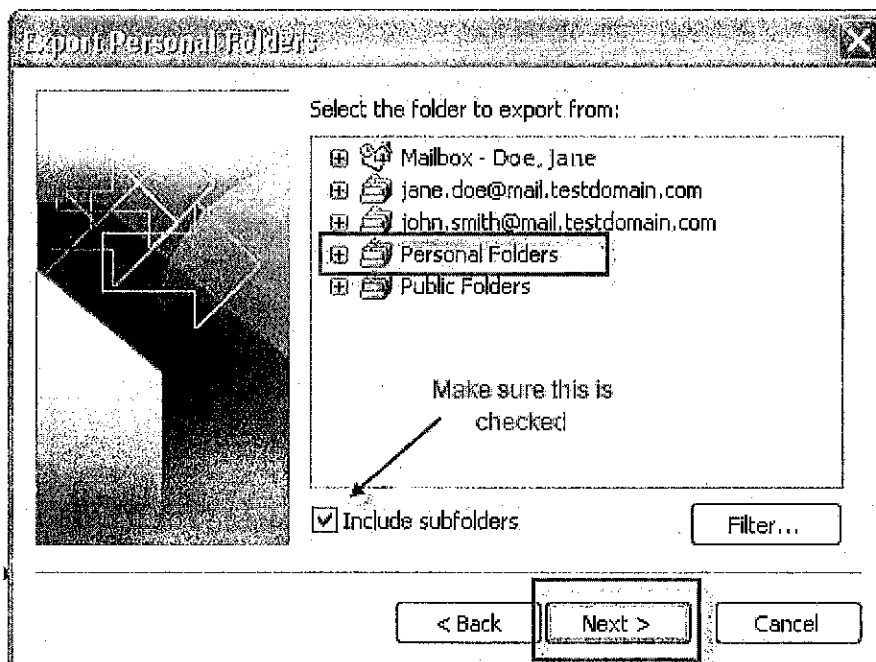
- As previously mentioned, by default, Outlook data files are saved on your local drive at: *drive: \Documents and Settings\user\Local Settings\Application Data\Microsoft\Outlook*. If you need to save the data file to your agency's network (for example, your supervisor needs access to the data file) or another location on your local hard drive, you will need to export the .pst to this new location.
- In Microsoft Outlook, highlight your Personal Folders folder. From the toolbar, select **File** → **Import and Export**.
- The Import and Export Wizard will appear. From the list, select "Export to a file" and then click **Next**.



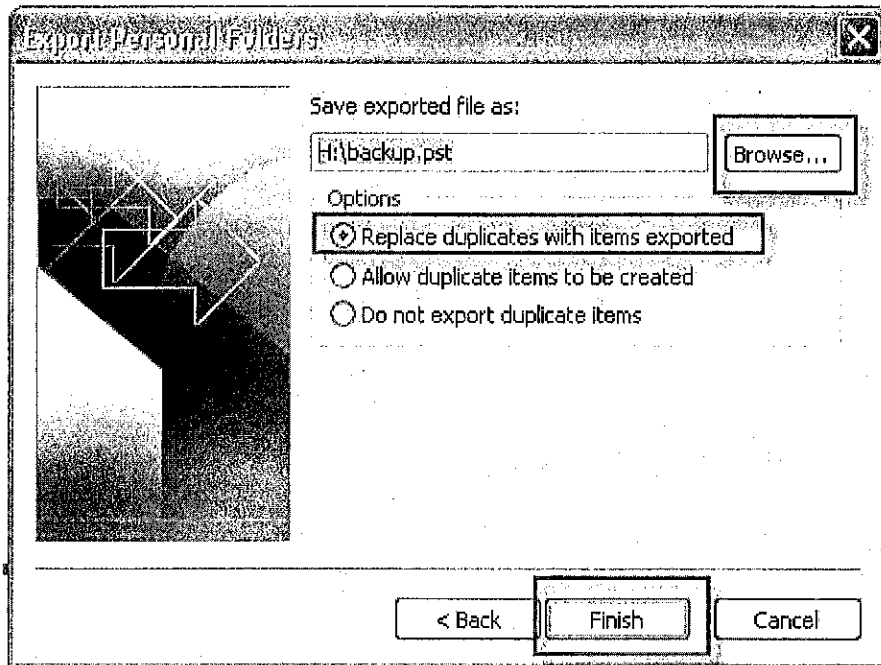
- On the next screen, select "Personal Folder File" (.pst) and then click **Next** (see next page).



- On the next screen, select the folder you want to export (in this case the Personal Folders folder). Be sure to check the Include subfolders option at the bottom. Click **Next**.



- On the next screen, click the **Browse** button, and then navigate to a location on your network drive or your local hard drive. Type in a file name, and then select OK. This will bring you back to the wizard screen. Under options, select how you want the duplicate items to be handled. To keep things simple, it is recommended you select "Replace duplicates with items exported." Click **Finish** at the bottom of the screen.



- A Create Microsoft Personal Folders window appears. If all the information looks correct, click the **OK** button at the bottom of the screen.
- Note that you can run this wizard as necessary. Just remember as a last step to replace duplicates with items exported, unless you want multiple copies of exports.

## Bibliography

Flynn, Nancy and Randolph Kahn Esq. 2003. *E-Mail Rules: A Business Guide to Managing Policies, Security, and Legal Issues*. New York: AMACOM (American Management Association).

Kentucky Department for Libraries and Archives. *Guidelines for Managing E-Mail in Kentucky Government*. <http://www.kdla.ky.gov/recmanagement/EmailGuidelines.pdf> (accessed February 25, 2009).

Montgomery, Haley. *How to Compose a Professional Business E-mail*. eHow.com. [http://www.ehow.com/how\\_4471941\\_compose-professional-business-email.html](http://www.ehow.com/how_4471941_compose-professional-business-email.html) (accessed March 1, 2009).

Nordquist, Richard. *Ten Tips on How to Write a Professional E-mail*. About.com. <http://grammar.about.com/od/developingessays/a/profemails.htm> (accessed March 1, 2009).

Pennock, Maureen. 2006. *Digital Curation Manual. Curating E-Mails: A life-cycle approach to the management and preservation of e-mail messages*. Digital Curation Centre. <http://www.dcc.ac.uk/resource/curation-manual/chapters/curating-e-mails/> (accessed February 25, 2009).

Privacy Right Clearinghouse. 2005. *Watch Out for "Phishing" E-mails: Attempting to Capture Your Personal Information*. <http://www.privacyrights.org/ar/phishing.htm> (accessed February 28, 2009).